SPYWOLF

Security Audit Report

Completed on

July 12, 2022

MADE IN USA 🇺🇸

SPYWOLF.CO
@SPYWOLFNETWORK
@SPYWOLFNETWORK

OVERVIEW

This audit has been prepared for **RemeDao** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

RemeDao

PROJECT DESCRIPTION

According to their whitepaper:

The RemeDAO will be rebase token system which will pay holders compounded rewards Everyday. In the DAO, users can propose and vote for their favorite meme tokens. The most vote token will be bought and distributed automatically by the RemeDAO system right after the voting end.

Release Date: Presale starts on July, 2022

Category: Rebase/DAO

CONTRACT INFO

Token Name
RemedaoV2

Symbol
RMD2

Contract Address
0xfC4A124Ab707762ec5FdE68aF7dc44b37208C5d2

Network
Binance Smart Chain

Language
Solidity

Deployment Date
July 09, 2022

Verified?
Yes

Total Supply
1,500,000

Status
Not launched

TAXES

Buy Tax
10%

Sell Tax
10%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

CURRENT STATS

(As of July 11, 2022)

Liquidity

Not added yet

Burn

No burnt tokens

Status:

Not Launched!

MaxSellTxAmount

10% of holder's balance per day

DEX:

PancakeSwap

LP Address(es)

Liquidity not added yet

TOKEN TRANSFERS STATS

Transfer Count	3
Uniq Senders	1
Uniq Receivers	3
Total Amount	1500000 RMD2
Median Transfer Amount	500000 RMD2
Average Transfer Amount	500000 RMD2
First transfer date	2022-07-09
Last transfer date	2022-07-09
Days token transferred	1

SMART CONTRACT STATS

Calls Count	1
External calls	1
Internal calls	0
Transactions count	1
Uniq Callers	1
Days contract called	1
Last transaction time	2022-07-09 05:04:48 UTC
Created	2022-07-09 05:04:48 UTC
Create TX	0x4cd4b02aab6718ac56cfccd73a28badd83341e29c075874ced72f4147755c297
Creator	0x50041bf8030210d67316048072e3079a884bf690

FEATURED WALLETS

***Owner address**	0x50041bf8030210d67316048072e3079a884bf690
***Insurance fund receiver**	0x4444d2a65d1f75f56f8b9d3f4d3fe55631bd6666
***Treasury receiver**	0x0000a9fdb9d4f7949d5b8060e4e93c7107729999
***Offchain game receiver**	0x6666b7426c5b2437FeB18359387CAF6251B1aaaa
LP address	**Liquidity not added yet**

*Address can be changed in future

TOP 3 UNLOCKED WALLETS

1 52% Same as treasury receiver

0x000000000000000000000000000000000000dead 33% 2

3 15% 0x0000000000000000000000000000000000000001

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

Users that participate in votes for new meme token, cannot sell their tokens in the current epoch.

```
function vote(address _erc20TokenAddress, uint256 epoch) public {
    require(epoch == lastVotingEpoch);
    require(!lockVote[epoch][msg.sender], "Lock vote");
    lockVote[epoch][msg.sender] = true;
.....................
}

function makeVote(address _erc20TokenAddress) external {
.............
    lockVote[epoch][msg.sender] = true;
.............
}

function _transferFrom(
    address sender,
    address recipient,
    uint256 amount
) internal returns (bool) {
.............
require(!lockVote[epoch][sender]);
.............
}
```

FOUND THREATS

⚠ Medium Risk

There are tokens minted into the offChainGameReceiver address after each rebase if burn address hold certain amount of tokens.
Owner can change offChainGameReceiver address to any address.

```
function setFeeReceivers(address _treasuryReceiver,
    address _insuranceFundReceiver, address _offChainGameReceiver
) external onlyOwner {
    treasuryReceiver = _treasuryReceiver;
    insuranceFundReceiver = _insuranceFundReceiver;
    offChainGameReceiver = _offChainGameReceiver;
}

function rebase() internal {
.......
autoTransferToOffchainGame();
......
}

function autoTransferToOffchainGame() internal {
    if (balanceOf(DEAD) > deadMaxBalance) {
        uint256 _maxGonLockBalance = deadMaxBalance.mul(gonsPerFragment);
        if (_gonBalances[DEAD] > _maxGonLockBalance) {
            uint256 gonTransferAmount = _gonBalances[DEAD].sub(
                _maxGonLockBalance
            );
            emit Transfer(
                DEAD,
                offChainGameReceiver,
                gonTransferAmount.div(gonsPerFragment)
            );
            _gonBalances[offChainGameReceiver] = _gonBalances[
                offChainGameReceiver
            ].add(gonTransferAmount);
            _gonBalances[DEAD] = _maxGonLockBalance;
            _updateAccountSnapshot(DEAD);
            _updateAccountSnapshot(offChainGameReceiver);
        }
    }
}
```

FOUND THREATS

⚠ Medium Risk

This is rebase token with changing supply up to 12,000,000,000.
Current supply is 1,500,000.
Rebase tokens can lead to price inflation over time.
Owner can turn on/off rebase.

```
uint256 public _maxSupply = 12 * 10**9 * 10**DECIMALS;

function setAuto(bool autoRebase, bool autoSwapBack) external onlyOwner {
    _autoRebase = autoRebase;
    _autoSwapBack = autoSwapBack;
}

function shouldRebase() internal view returns (bool) {
    uint256 epoch = currentRebaseEpoch();
    return
        isStartRebase &&
        _autoRebase &&
        msg.sender != pair &&
        !inSwap &&
        epoch > _rebaseEpoch &&
        _totalSupply < _maxSupply;
}
```

FOUND THREATS

⚠ Medium Risk

Owner can exclude address from taxes and max sell limit.

```
function setWhitelist(address _addr, bool _flag) external onlyOwner {
    _isFeeExempt[_addr] = _flag;
}

function _transferFrom(
    address sender, address recipient, uint256 amount
) internal returns (bool) {

if (recipient == pair && !_isFeeExempt[sender]) {
.....................................
    if (maxSellInEpoch[sender][epoch] == 0) {
        maxSellInEpoch[sender][epoch] = _gonBalances[sender];
    }
    require(
        sell[sender][epoch].add(gonAmount) <=
            maxSellInEpoch[sender][epoch].mul(maxSell).div(
                maxSellDenominator
            )
    );
    sell[sender][epoch] = sell[sender][epoch].add(gonAmount);
}

 uint256 gonAmountReceived = shouldTakeFee(sender, recipient) ?
    takeFee(sender, gonAmount) : gonAmount;
.....................................
}

function shouldTakeFee(address from, address to)
    internal view returns (bool){
    return (pair == from || pair == to) && !_isFeeExempt[from];
}
```

FOUND THREATS

⚠ Low Risk

Owner can change buy/sell fees up to 11% (combined buy+sell=22%).

```
uint256 public constant feeDenominator = 1000;

function setFee(
    uint256 _treasuryFee,
    uint256 _insuranceFundFee,
    uint256 _memeFee
) external onlyOwner {
    require(_treasuryFee + _insuranceFundFee + _memeFee < 120);
    treasuryFee = _treasuryFee;
    insuranceFundFee = _insuranceFundFee;
    memeFee = _memeFee;
    totalFee = treasuryFee.add(insuranceFundFee).add(memeFee);
}

function takeFee(address sender, uint256 gonAmount)
internal returns (uint256) {
    int256 feeAmount = gonAmount.mul(totalFee).div(feeDenominator);
.....
}
```

FOUND THREATS

⚠ Low Risk

Owner can change the minimum tokens criteria to participate in votes.

```
uint256 public constant minMakeVoteDenominator = 100_000;

function setMinMakeVote(uint256 _minMakeVote) external onlyOwner {
    require(_minMakeVote <= 10000);
    minMakeVote = _minMakeVote;
}

function minTokenToVote() external view returns (uint256) {
    return _totalSupply.mul(minMakeVote).div(minMakeVoteDenominator);
}
```

FOUND THREATS

Informational

Owner can blacklist only contract addresses (LP excluded).

```
function setBotBlacklist(address _botAddress, bool _flag)
    external
    onlyOwner
{
    require(
        Address.isContract(_botAddress) && _botAddress != pair,
        "only contract address"
    );
    blacklist[_botAddress] = _flag;
}
```

Owner can change the minimum tokens criteria to participate in votes.

```
uint256 public constant minMakeVoteDenominator = 100_000;

function setMinMakeVote(uint256 _minMakeVote) external onlyOwner {
    require(_minMakeVote <= 10000);
    minMakeVote = _minMakeVote;
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

RemeDao

GOOD PRACTICES FOUND

- ✔ The smart contract utilizes "SafeMath" to prevent overflows

This is 1:1 migration from the previous version of the token. There is no info about the initial tokens distribution for presale.

TOKENOMICS

THE TEAM

The team at **RemeDao** has privately doxxed to SPYWOLF by completing the following KYC requirements:

- ID Verification
- Video statement
- Video interview with devs
- Owner's wallet verification

KYC INFORMATION

Issuer

SPYWOLF

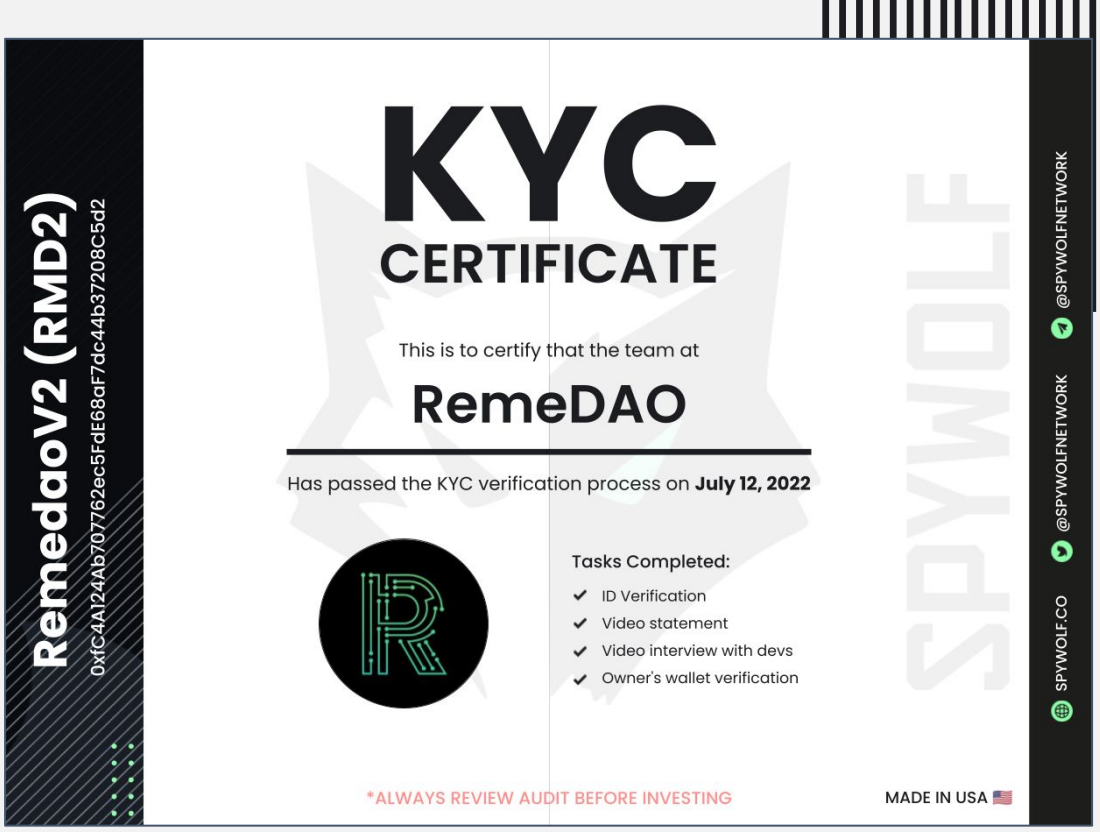
Members

KYC Date

July 12, 2022

Format

Image



Certificate Link

https://github.com/SpyWolfNetwork/KYCs/blob/main/July/KYC_ReMeDAO_0xfC4A124Ab707762ec5FdE68aF7dc44b37208C5d2.png

WEBSITE

Website URL
https://remedao.com/

Domain Registry
https://www.namesilo.com/

Domain Expiration
Expires on 2023-06-12

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

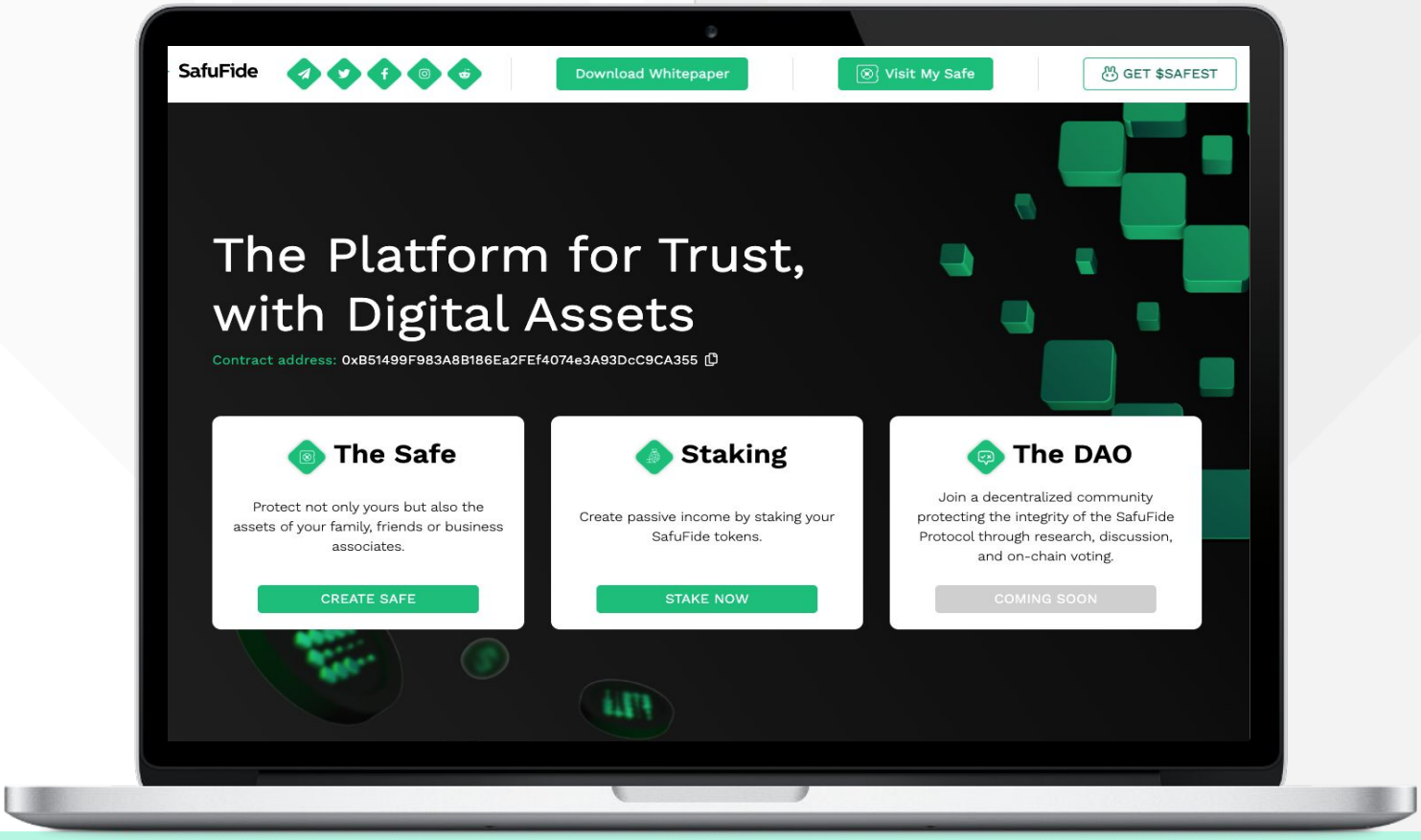
Design
Single page design, appropriate color scheme.

Content
Informational, no grammar mistakes.

Whitepaper
Well written, explanatory.

Roadmap
Yes, goals set at 4 phases without time frames.

Mobile-friendly?
Yes



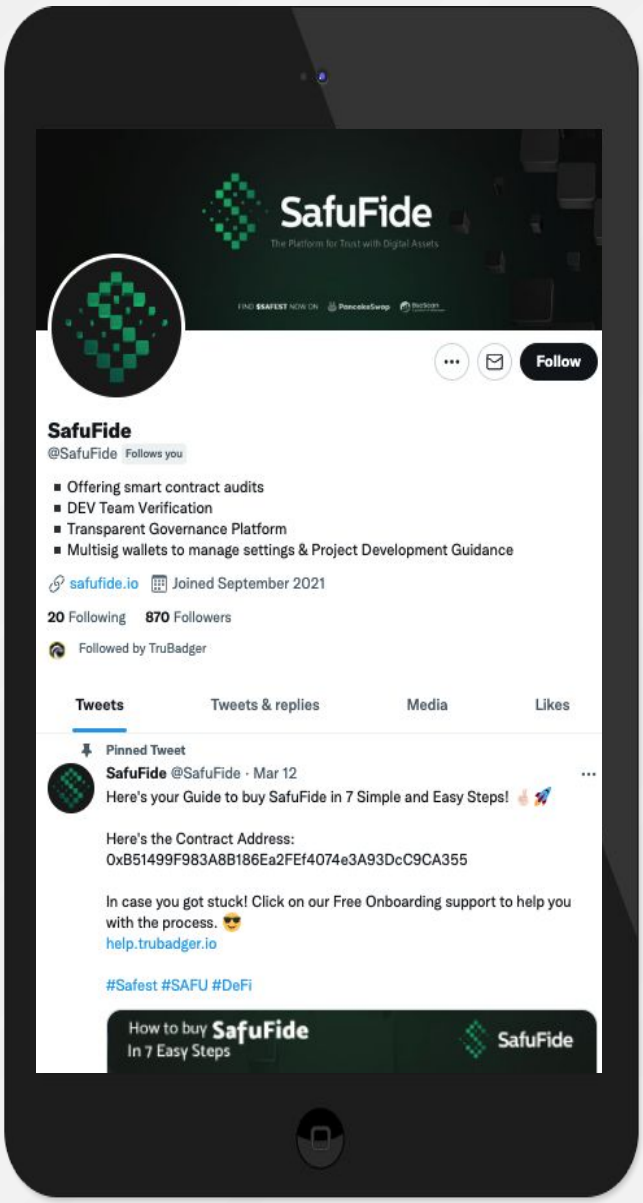
remedao.com

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media activity is moderate. They did a good job communicating to their community about their contract migration.



Twitter

https://twitter.com/RemeDAOBSC

- 9 904 followers
- Active

Discord

- Not available

Telegram

https://t.me/RemeDAOBSC

- 16 005 members
- Few active members
- Active mod

Medium

https://medium.com/@RemeDAO

- 6 total articles

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 150 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

SPYWOLF.NETWORK

@SPYWOLFNETWORK

@SPYWOLFOFFICIAL

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.